

ON DISTINCT PERPENDICULAR BISECTORS AND PINNED DISTANCES IN FINITE FIELDS

BRANDON HANSON, BEN LUND AND OLIVER ROCHE-NEWTON

ABSTRACT. Given a set of points $P \subset \mathbb{F}_q^2$ such that $|P| \geq q^{4/3}$, we establish that for a positive proportion of points $\mathbf{a} \in P$, we have

$$|\{\|\mathbf{a} - \mathbf{b}\| : \mathbf{b} \in P\}| \gg q,$$

where $\|\mathbf{a} - \mathbf{b}\|$ is the distance between points \mathbf{a} and \mathbf{b} . This improves a result of Chapman et al. [6].

A key ingredient of our proof also shows that, if $|P| \geq q^{3/2}$, then the number B of distinct lines which arise as the perpendicular bisector of two points in P satisfies $B \gg q^2$.

1. INTRODUCTION

Given a set of points P , it is natural to construct a set of lines by connecting distinct pairs of elements from P . Roughly speaking, one expects that this set of lines determined by P should be large, unless the point set is highly collinear. A seminal result of this kind was Beck's Theorem [3], which established that there exist absolute constants $c, k > 0$ such that if $P \subset \mathbb{R}^2$, then either P determines $c|P|^2$ distinct lines, or there exists a single line supporting $k|P|$ points from P . Different versions of Beck's Theorem for the finite field¹ setting, in which we begin by considering a point set $P \subset \mathbb{F}_q^2$, have been proven in [1, 8, 10].

In this paper, we consider an alternative take on Beck's theorem, in which we look at the set of perpendicular bisectors determined by a point set $P \subset \mathbb{F}_q^2$. For a vector $\mathbf{x} = (x_1, x_2) \in \mathbb{F}_q^2$, we define $\|\mathbf{x}\| = x_1^2 + x_2^2$ and call $\|\mathbf{x} - \mathbf{y}\|$ the *distance* between \mathbf{x} and \mathbf{y} . Though it is not actually a metric since it takes values in \mathbb{F}_q , this notion of distance shares a number of purely algebraic properties with the Euclidean distance. Given two distinct points $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^2$, we define the *perpendicular bisector of \mathbf{a} and \mathbf{b}* to be the set

$$B(\mathbf{a}, \mathbf{b}) := \{\mathbf{c} \in \mathbb{F}_q^2 : \|\mathbf{c} - \mathbf{a}\| = \|\mathbf{c} - \mathbf{b}\|\}.$$

It is a simple calculation to check that $B(\mathbf{a}, \mathbf{b})$ is indeed a line in \mathbb{F}_q^2 . Now, define $B(P)$ to be the set of all perpendicular bisectors determined by pairs

Date: August 1, 2016.

Key words and phrases. finite fields, perpendicular bisectors, pinned distances, isosceles triangles, rigid motions, expander mixing lemma.

¹Whenever we refer to a field \mathbb{F}_q in this paper, it is assumed that the field has characteristic strictly greater than 2.

of points from P with non-zero distance. That is,

$$B(P) := \{B(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in P, \|\mathbf{a} - \mathbf{b}\| \neq 0\}.$$

Again, we expect that $|B(P)|$ will be large, provided that P is not of some degenerate form. One of these degenerate cases occurs when the point set P consists of many points on the same line. If all of the points lie on the same line, it is possible that $|B(P)|$ could be as small as $2|P| - 3$. Another degenerate case occurs when the points of P are equidistributed on a circle. However, these constructions only seem to work for relatively small point sets. Indeed the points on a line or circle are contained in a one-dimensional subset of the plane. In this paper we prove that provided a point set is sufficiently large, a positive proportion of all lines arise as perpendicular bisectors:

Theorem 1. *If $P \subset \mathbb{F}_q^2$ such that $|P| \geq q^{3/2}$, then*

$$|B(P)| \gg q^2.$$

In concurrent work, Lund, Sheffer and de Zeeuw proved an analog to Theorem 1 for finite sets of points in the real plane [12].

Theorem 1 was partly motivated by an application for the “pinned distance problem” in \mathbb{F}_q^2 . The aim of this problem is to show that, for any given point set, there always exists a point (or indeed many points) from the set which determines many distances with the rest of the point set. One of the key ingredients used to prove Theorem 1 can be combined with an incidence theorem for multisets of points and lines in order to establish the following result:

Theorem 2. *Let $P \subset \mathbb{F}_q^2$ such that $|P| \geq q^{4/3}$. Then there exists a subset $P' \subset P$ such that $|P'| \gg |P|$ and for all $\mathbf{a} \in P'$ we have the estimate*

$$(1) \quad |\{\|\mathbf{a} - \mathbf{b}\| : \mathbf{b} \in P\}| \gg q.$$

To give some context for Theorem 2, we refer to the work of Chapman et al. (see [6, Theorem 2.3]), who proved that for a point set $P \subset \mathbb{F}_q^d$ with $|P| \geq q^{\frac{d+1}{2}}$, there exists a subset $P' \subset P$ such that $|P'| \gg |P|$ and for all $\mathbf{x} \in P'$, (1) holds. Theorem 2 gives an improvement on this result in the case when $d = 2$.

The pinned distance problem is a variant on the classical Erdős “distinct distance problem”, and a trivial observation is that a lower bound for pinned distances implies a lower bound for the number of distinct distances determined by a set. In the real plane, the distinct distance problem was almost completely resolved by Guth and Katz [7], whilst the harder pinned distance problem remains wide open. The sequence of works in [4, 9] established that a set of $q^{4/3}$ points in \mathbb{F}_q^2 determines a positive proportion of the q distinct distances. With Theorem 2, the threshold for the number of points in the plane that will necessarily determine a positive proportion of all pinned distances now matches that known for distances.

Both Theorem 1 and Theorem 2 are deduced from a bound on the number of pairs of pairs of points that determine the same line as a bisector. For a point set $P \subseteq \mathbb{F}_q^2$, define the set

$$Q(P) := \{(x, y, z, w) \in P^4 : B(x, z) = B(y, w), \|x - z\| \neq 0\}.$$

When the point set P is obvious from the context, we will sometimes drop the argument and simply write Q instead of $Q(P)$.

Theorem 3. *For $P \subset \mathbb{F}_q^2$,*

$$|Q(P)| \ll \frac{|P|^4}{q^2} + q|P|^2.$$

It is interesting to note that, while we don't believe that Theorems 1 or 2 are tight, Theorem 3 is tight up to the implicit constants. A randomly chosen set of points shows that it is possible to construct a set $P \subset \mathbb{F}_q^2$ for which $|Q| \gg |P|^4/q^2$, and hence Theorem 3 is tight when $|P| \gg q^{3/2}$. Suppose now that P consists of the union of $|P|/q$ parallel lines, each containing q points. Now let l be a line perpendicular to these lines. Then l is the bisector of $|P|$ pairs of points in P - each line contains q pairs of points with l as their bisector. In particular, the number of pairs (x, z) and (y, w) each with l as their bisector is $|P|^2$. There are q lines l which are perpendicular to the lines defining P , so $|Q| \geq |P|^2 q$; this shows that Theorem 3 is tight when $|P| \ll q^{3/2}$.

Note that in the definitions of the sets $B(P)$ and $Q(P)$, we make the point of excluding pairs of points whose distance is zero. These can arise if the element $-1 \in \mathbb{F}_q$ has a square root in \mathbb{F}_q , which happens exactly when q is congruent to 1 modulo 4. The possibility of points with zero distances present some extra technical difficulties in the forthcoming analysis, and it is often necessary to consider separately the cases when q is congruent to either 1 or 3 modulo 4. In fact, Theorem 3 would not be true if quadruples arising from such zero distances were included in the set Q . It can be calculated that if P is the union of $|P|/q$ isotropic lines, then we would have $|P|q^3$ quadruples since any four points x, y, z, w on an isotropic line satisfy $B(x, z) = B(y, z)$. The arguments in this paper when $q \equiv 3 \pmod{4}$ are slightly more straightforward, since zero distances are not an issue in this case.

The rest of the paper is structured as follows. In section 2 we go over preliminary results needed. We cover some simple plane geometry over finite fields in subsection 2.1. We will quote a number of elementary results from finite plane geometry, though we leave the proofs to an appendix in the interest of brevity. If the reader is familiar with plane geometry, these results will be quite believable. In subsection 2.2, we record a version of the Expander Mixing Lemma, also proved in an appendix, and recall a few facts we will need from linear algebra. We prove Theorem 3, and consequently Theorem 1, in section 3. Finally, in section 4, we record a version of the finite

field Szemerédi-Trotter theorem for multisets, and combine this incidence result with Theorem 3 in order to prove Theorem 2.

The methods used are a combination of elementary geometry and spectral graph theory. It is likely that Fourier analysis (i.e. the use of exponential sums) would succeed just as well in proving our theorems, but we have instead chosen to work with graphs, which maintains the combinatorial spirit of the problem.

Notation. We recall that the notations $U \ll V$ and $V \gg U$ are both equivalent to the statement that the inequality $|U| \leq cV$ holds with some constant $c > 0$.

2. PRELIMINARIES

2.1. Results from Finite Plane Geometry. In this section we establish a few facts from finite planar geometry. For proofs of the facts claimed in this section we refer to Appendix A.

Recall the notion of distance introduced earlier; when $\mathbf{x} = (x_1, x_2), \mathbf{y} = (y_1, y_2) \in \mathbb{F}_q^2$ we will write

$$\mathbf{x} \cdot \mathbf{y} = \mathbf{x}^t \mathbf{y}$$

for the standard inner product and

$$\|\mathbf{x}\| = \mathbf{x} \cdot \mathbf{x}.$$

This is not a distance in usual sense since the elements of \mathbb{F}_q are not sensibly ordered, but many of properties of a norm persist in an algebraic fashion. The set of points a fixed distance from a given point is a circle

$$C_r(\mathbf{u}) = \{\mathbf{x} \in \mathbb{F}_q^2 : \|\mathbf{x} - \mathbf{u}\| = r\}.$$

We call \mathbf{u} the centre of the circle and r the radius. We remark here that when $q \equiv 1 \pmod{4}$ then there is an element $i \in \mathbb{F}_q$ satisfying $i^2 = -1$ and so there are non-zero points on the circle of zero radius. Recall that the bisector of two distinct points \mathbf{x} and \mathbf{y} , is denoted as

$$B(\mathbf{x}, \mathbf{y}) := \{\mathbf{c} \in \mathbb{F}_q^2 : \|\mathbf{c} - \mathbf{x}\| = \|\mathbf{c} - \mathbf{y}\|\}.$$

Equivalently, the bisector of \mathbf{x} and \mathbf{y} is the line passing through the midpoint $\frac{1}{2}(\mathbf{x} + \mathbf{y})$ with direction orthogonal to $\mathbf{x} - \mathbf{y}$.

We will use the symmetries of the plane to understand the distribution of bisectors.

Definition (Rotations, Reflections and Translations). *A matrix of the form*

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad a^2 + b^2 = 1$$

is called a rotation matrix, and a matrix of the form

$$\begin{pmatrix} a & b \\ b & -a \end{pmatrix}, \quad a^2 + b^2 = 1$$

is called a reflection matrix. If $\mathbf{u} \in \mathbb{F}_q^2$ and R is a rotation matrix, then a rotation about \mathbf{u} by R is an affine map of the form

$$\mathcal{R}(\mathbf{v}) = \mathcal{R}_{R,\mathbf{u}}(\mathbf{v}) = R(\mathbf{v} - \mathbf{u}) + \mathbf{u}.$$

If $\mathbf{u} \in \mathbb{F}_q^2$ and S is a reflection matrix, then a reflection about \mathbf{u} by S is an affine map of the form

$$\mathcal{S}(\mathbf{v}) = \mathcal{S}_{S,\mathbf{u}}(\mathbf{v}) = S(\mathbf{v} - \mathbf{u}) + \mathbf{u}.$$

A translation by \mathbf{u} is an affine map of the form

$$\mathcal{T}(\mathbf{v}) = \mathcal{T}_{\mathbf{u}}(\mathbf{v}) = \mathbf{v} + \mathbf{u}.$$

For our purposes we need the connection between reflections and bisectors. However, it is not the case that all lines arise as the fixed line of a reflection. Indeed, we need to account for the possibility of elements with vanishing norm. A line l is called *isotropic* if it is of the form

$$l = \{t \cdot (1, \pm i) + \mathbf{u} : t \in \mathbb{F}_q\}$$

where $i^2 = -1$. With these definitions, we are now ready to state four lemmas which will be used towards proving the results on distinct bisectors and pinned distances.

Lemma 4. *If $\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w} \in \mathbb{F}_q^2$ are such that $B = B(\mathbf{x}, \mathbf{z}) = B(\mathbf{y}, \mathbf{w})$ is non-isotropic then $\|\mathbf{x} - \mathbf{y}\| = \|\mathbf{z} - \mathbf{w}\|$.*

Lemma 5. *There are $q + 1$ lines passing through any $\mathbf{u} \in \mathbb{F}_q^2$.*

- (1) *If $q \equiv 1 \pmod{4}$ then two of the lines are isotropic and $q - 1$ are non-isotropic. It follows that there are $q - 1$ rotations and reflections about any point \mathbf{u} .*
- (2) *When $q \equiv 3 \pmod{4}$ all lines are non-isotropic. It follows that there are $q + 1$ rotations and reflections about any point \mathbf{u} .*

Lemma 6. *Suppose $\mathbf{u} \in \mathbb{F}_q^2$ and $r \in \mathbb{F}_q$. Then we have:*

- (1) *$|C_r(\mathbf{u})| = q - 1$ if $r \neq 0$ and $|C_0(\mathbf{u})| = 2q - 1$ whenever $q \equiv 1 \pmod{4}$;*
- (2) *$|C_r(\mathbf{u})| = q + 1$ if $r \neq 0$ and $|C_0(\mathbf{u})| = 1$ whenever $q \equiv 3 \pmod{4}$.*

It follows that the number of ordered pairs $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_q^2 \times \mathbb{F}_q^2$ with $\|\mathbf{x} - \mathbf{y}\| = r$ is:

- (1) *$q^2(q - 1)$ if $r \neq 0$ and $q^2(2q - 1)$ if $r = 0$ whenever $q \equiv 1 \pmod{4}$;*
- (2) *$q^2(q + 1)$ if $r \neq 0$ and q^2 if $r = 0$ whenever $q \equiv 3 \pmod{4}$.*

Lemma 7. *Suppose $\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w} \in \mathbb{F}_q^2$ are such that $(\mathbf{x}, \mathbf{y}) \neq (\mathbf{z}, \mathbf{w})$ and*

$$\|\mathbf{x} - \mathbf{y}\| = \|\mathbf{z} - \mathbf{w}\| \neq 0.$$

If $\mathbf{x} - \mathbf{y} \neq \mathbf{z} - \mathbf{w}$, then there are $q - 1$ pairs of reflections $(\mathcal{R}_1, \mathcal{R}_2)$ with $\mathcal{R}_1(\mathbf{x}) = \mathcal{R}_2(\mathbf{z})$ and $\mathcal{R}_1(\mathbf{y}) = \mathcal{R}_2(\mathbf{w})$ when $q \equiv 1 \pmod{4}$ and $q + 1$ such pairs when $q \equiv 3 \pmod{4}$. If $\mathbf{x} - \mathbf{y} = \mathbf{z} - \mathbf{w}$ and $\|\mathbf{x} - \mathbf{z}\| \neq 0$, then there are q such pairs of reflections. If $\mathbf{x} - \mathbf{y} = \mathbf{z} - \mathbf{w}$ and $\|\mathbf{x} - \mathbf{z}\| = 0$, then there are no such pairs of reflections.

2.2. Some Linear Algebra and the Expander Mixing Lemma. Here, we recall some simple facts we need from linear algebra. The main tool we use in our arguments is the Expander Mixing Lemma, a standard result in spectral graph theory [2]. In fact we need a weighted variant of the lemma for the results coming in Sections 3 and 4.

Suppose G is a δ -regular graph, meaning each vertex in G is adjacent to δ other vertices. If A is the adjacency matrix of G , note that the largest eigenvalue of A is δ ; the eigenvector corresponding to this eigenvalue is the all-1s vector. We let $L^2(V)$ be the set of complex valued functions on the vertex set V endowed with the inner product

$$\langle f, g \rangle = \sum_{v \in V} f(v) \bar{g}(v)$$

and norm

$$\|f\|^2 = \langle f, f \rangle.$$

The matrix A acts on $L^2(V)$ by the formula

$$Af(v) = \sum_{\{u,v\} \in E} f(u).$$

Finally, we let \mathbb{E} denote the expectation:

$$\mathbb{E}(f) = \frac{1}{|V|} \sum_{v \in V} f(v).$$

We recall here the following versions of the Plancherel and Parseval identities.

Lemma 8. *Let B be an orthonormal basis for $L^2(V)$. Then we have*

$$\sum_{v \in V} |f(v)|^2 = \sum_{b \in B} |\langle f, b \rangle|^2$$

and

$$\sum_{v \in V} f(v) \bar{g}(v) = \sum_{b \in B} \langle f, b \rangle \langle b, g \rangle.$$

We have the following version of the expander mixing lemma. The proof is postponed to Appendix B.

Lemma 9 (Expander Mixing Lemma). *Let $G = (V, E)$ be a δ -regular graph with $|V| = n$, and let A be the adjacency matrix for G . Suppose the absolute values of all but the largest eigenvalue of A are bounded by λ . Suppose $f, g \in L^2(V)$, then*

$$|\langle f, Ag \rangle - \delta n \mathbb{E}(f) \mathbb{E}(g)| \leq \lambda \|f\| \|g\|.$$

In particular, let $S, T \subseteq V$, and denote by $E(S, T)$ the number of edges between S and T . Then,

$$|E(S, T) - \delta |S| |T| / n| \leq \lambda \sqrt{|S| |T|}.$$

Finally we will also need the following standard fact from linear algebra.

Lemma 10 (Gershgorin Circle Theorem). [5] *Let $A = [A_{ij}]$ be an $n \times n$ matrix, and let $r_i = \sum_{j=1}^n |a_{ij}|$ be the sum of the absolute values of the i^{th} row of A . Then each eigenvalue of A is contained in at least one of the disks*

$$\mathcal{D}_i = \{z : |z - a_{ii}| \leq r_i\}$$

in the complex plane.

3. DISTINCT PERPENDICULAR BISECTORS

In this section, we will prove Theorems 1 and 3. The basic approach is to associate our problem with a graph, and then use the facts about rigid motions from Section 2.1 to analyze the eigenvalues of this graph, so that we can apply the expander mixing lemma.

It will be more convenient to deduce Theorem 3 from the following similar result:

Lemma 11. *For a point set $P \subseteq \mathbb{F}_q^2$, define the set*

$$Q'(P) := \{(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) \in P^4 : B(\mathbf{x}, \mathbf{z}) = B(\mathbf{y}, \mathbf{w}), \|\mathbf{x} - \mathbf{y}\| \neq 0\}.$$

Then

$$|Q'(P)| \ll \frac{|P|^4}{q^2} + q|P|^2.$$

Note that, although Lemma 11 appears very similar to Theorem 3, they are not identical. In the definition of $Q(P)$ quadruples for which $\|\mathbf{x} - \mathbf{z}\| = 0$ are excluded, whereas the definition of $Q'(P)$ excludes quadruples for which $\|\mathbf{x} - \mathbf{y}\| = 0$. First we deduce Theorem 3 from Lemma 11.

Proof of Theorem 3 from Lemma 11. Define the sets

$$\begin{aligned} Q' &= Q_1 := \{(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) : B(\mathbf{x}, \mathbf{z}) = B(\mathbf{y}, \mathbf{w}), \|\mathbf{x} - \mathbf{y}\| \neq 0\}, \\ Q_2 &:= \{(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) : B(\mathbf{x}, \mathbf{z}) = B(\mathbf{y}, \mathbf{w}), \|\mathbf{x} - \mathbf{w}\| \neq 0\}, \\ Q_3 &:= \{(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) : B(\mathbf{x}, \mathbf{z}) = B(\mathbf{y}, \mathbf{w}), \|\mathbf{z} - \mathbf{y}\| \neq 0\}, \\ Q_4 &:= \{(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) : B(\mathbf{x}, \mathbf{z}) = B(\mathbf{y}, \mathbf{w}), \|\mathbf{z} - \mathbf{w}\| \neq 0\}. \end{aligned}$$

Note that $|Q_1| = |Q_2| = |Q_3| = |Q_4|$, since there is a natural bijection between Q_i and Q_j for any $1 \leq i, j \leq 4$. Therefore,

$$|Q| \ll |Q'| + |Q \setminus (Q_1 \cup Q_2 \cup Q_3 \cup Q_4)|.$$

It remains to bound the size of the set $Q \setminus (Q_1 \cup Q_2 \cup Q_3 \cup Q_4) := Q''$.

Let \mathbf{x} and \mathbf{z} be arbitrary elements from P such that $\|\mathbf{x} - \mathbf{z}\| \neq 0$. We will show that there are at most two pairs (\mathbf{y}, \mathbf{w}) such that $(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) \in Q''$. Indeed, if $(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) \in Q''$ then we have

$$(2) \quad \|\mathbf{x} - \mathbf{y}\| = \|\mathbf{x} - \mathbf{w}\| = \|\mathbf{z} - \mathbf{y}\| = \|\mathbf{z} - \mathbf{w}\| = 0.$$

It follows from (2) that \mathbf{y} and \mathbf{w} each lie on one of the two isotropic lines through \mathbf{x} . Similarly, \mathbf{y} and \mathbf{w} each lie on one of the two isotropic lines through \mathbf{z} . However, since $\|\mathbf{x} - \mathbf{z}\| \neq 0$, these four isotropic lines

are distinct. There are then only two possible choices for the pair (\mathbf{y}, \mathbf{w}) (including reordering the two elements).

Finally, we have $|Q''| \ll |P|^2$, and it then follows from Lemma 3 that

$$|Q| \ll |Q'| + |Q''| \ll \frac{|P|^4}{q^2} + q|P|^2 + |P|^2 \ll \frac{|P|^4}{q^2} + q|P|^2,$$

as required. \square

Fixed Distance Bisector Quadruples. We are now going to prove the main technical result from which we will deduce our results. We will split the set of bisector quadruples according to the distances between the pairs of points. The technical result, which proceeds by way of spectral graph theory, shows that the bisector quadruples at a given distance are distributed uniformly among all point pairs with this distance. Then we employ an estimate for distance quadruples and deduce a bound for bisector quadruples.

For the remainder of this section, let $P \subseteq \mathbb{F}_q^2$ be a fixed set of points. Recall that our immediate goal is to place an upper bound on the size of the set

$$Q' = Q'(P) = \{(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) \in P^4 : B(\mathbf{x}, \mathbf{z}) = B(\mathbf{y}, \mathbf{w}), \|\mathbf{x} - \mathbf{y}\| \neq 0\}.$$

Rather than bounding $|Q'|$ directly, we will partition Q' into subsets defined by pairs of points at a fixed distance. For each $d \in \mathbb{F}_q$, define

$$Q'_d = Q'_d(P) = \{(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) \in Q' : \|\mathbf{x} - \mathbf{y}\| = \|\mathbf{z} - \mathbf{w}\| = d\}, \text{ and}$$

$$\Pi_d = \Pi_d(P) = \{(\mathbf{x}, \mathbf{y}) \in P^2 : \|\mathbf{x} - \mathbf{y}\| = d\}.$$

From Lemma 4, we have

$$Q' = \bigcup_{d \neq 0} Q'_d.$$

The following result establishes the uniformity of bisector quadruples at distance d within all point pairs at distance d .

Proposition 12. *For $d \neq 0$,*

$$|Q'_d| \leq \frac{|\Pi_d|^2}{q} + 2(q-1)|\Pi_d|.$$

Proof. Let G be a graph with vertices

$$V = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_q^2 \times \mathbb{F}_q^2 : \|\mathbf{x} - \mathbf{y}\| = d\},$$

and edges

$$E = \{(\mathbf{x}, \mathbf{y}), (\mathbf{z}, \mathbf{w}) \in V^2 : B(\mathbf{x}, \mathbf{z}) = B(\mathbf{y}, \mathbf{w})\}.$$

For $x \in V$, define $\Gamma(x)$ to be the neighbourhood of x ; in other words,

$$\Gamma(x) = \{y \in V : \{x, y\} \in E\}.$$

Let A be the adjacency matrix of G . It is straightforward to see that $A_{xy}^2 = |\Gamma(x) \cap \Gamma(y)|$, the number of paths of length 2 from x to y in G .

The plan is to bound the second eigenvalue of A^2 , and use this along with Lemma 9 to complete the proof. We will bound the eigenvalues of A^2 separately in the cases $q \equiv 1 \pmod{4}$ and $q \equiv 3 \pmod{4}$. The method that we use to bound the eigenvalues in each case is reminiscent of the method used in [15].

Suppose first that $q \equiv 1 \pmod{4}$.

By Lemma 6, $|V| = q^2(q-1)$. Each vertex has an edge for each of the $q(q-1)$ non-isotropic lines, so G is a $q(q-1)$ -regular graph. From Lemma 7, we have

$$|\Gamma(x) \cap \Gamma(y)| = \begin{cases} q(q-1), & \text{if } x = y, \\ q, & \text{if } y \text{ is a non-isotropic translation of } x, \\ 0, & \text{if } y \neq x \text{ and } y \text{ is an isotropic translation of } x, \\ q-1, & \text{otherwise.} \end{cases}$$

Hence, we can write

$$A^2 = (q-1)J + (q-1)^2I + E,$$

where J is the all-1s matrix, I is the identity matrix, and $E = [E_{xy}]$ is a matrix such that

$$E_{xy} = \begin{cases} 1, & \text{if } y \text{ is a non-isotropic translation of } x, \\ 1-q, & \text{if } y \neq x \text{ and } y \text{ is an isotropic translation of } x, \\ 0, & \text{otherwise.} \end{cases}$$

Since E is real and symmetric, it has real eigenvalues. By Lemma 6, any fixed pair of points has $2(q-1)$ distinct non-trivial isotropic translations and $(q-1)^2$ distinct non-isotropic translations. Hence, the sum of the absolute values of the elements on each row of E is equal to $3(q-1)^2$; in other words, for any $1 \leq i \leq n$,

$$\sum_{j=1}^n |E_{ij}| = 3(q-1)^2.$$

Hence, by Lemma 10, the absolute value of each eigenvalue of E is bounded by $3(q-1)^2$.

Since A is a real symmetric matrix, its eigenvectors can be taken to be real and orthogonal. Moreover, because the row sums of A are all equal, the all-1s vector is an eigenvector of A .

Let \mathbf{v} be an eigenvector of A that is orthogonal to the all-1s vector and that has eigenvalue λ . It is clear that \mathbf{v} is an eigenvector of I with eigenvalue 1 and an eigenvector of J with eigenvalue 0. For any constants a, b , the vector \mathbf{v} is an eigenvector of the matrix $A^2 - aI - bJ$ with eigenvalue $\lambda^2 - a$. In particular, it is an eigenvector of the matrix $E = A^2 - (q-1)^2I - (q-1)J$ and (by above) its eigenvalue is at most $3(q-1)^2$.

Now we have $E\mathbf{v} = (\lambda^2 - (q-1)^2)\mathbf{v}$ and hence

$$|\lambda^2 - (q-1)^2| \leq 3(q-1)^2, \quad \text{so that} \\ \lambda^2 \leq 4(q-1)^2.$$

Hence, the absolute value of each eigenvalue of A that corresponds to an eigenvector orthogonal to the all-1s vector is bounded above by $2(q-1)$.

Now, suppose that $q \equiv 3 \pmod{4}$.

By Lemma 6, $|V| = q^2(q+1)$. Each vertex has an edge for each of the $q(q+1)$ lines, so G is a $q(q+1)$ -regular graph. From Lemma 7, we have

$$|\Gamma(x) \cap \Gamma(y)| = \begin{cases} q(q+1), & \text{if } x = y, \\ q, & \text{if } y \neq x \text{ and } y \text{ is a translation of } x, \\ q+1, & \text{otherwise.} \end{cases}$$

Hence, we can write

$$A^2 = (q+1)J + (q-1)(q+1)I + E,$$

where J is the all-1s matrix, I is the identity matrix, and $E = [E_{xy}]$ is a matrix such that

$$E_{xy} = \begin{cases} -1, & \text{if } y \neq x \text{ and } y \text{ is a translation of } x, \\ 0, & \text{otherwise.} \end{cases}$$

By Lemma 5, any fixed pair of points has $(q-1)(q+1)$ distinct non-trivial translations. Hence, the sum of the absolute values of the elements on each row of E is equal to $(q-1)(q+1)$; in other words, for any $1 \leq i \leq n$,

$$\sum_{j=1}^n |E_{ij}| = (q-1)(q+1).$$

Hence, by Lemma 10, the absolute value of each eigenvalue of E is bounded by $(q-1)(q+1)$.

Let \mathbf{v} be an eigenvector of A , orthogonal to the all-1s vector and associated with eigenvalue λ . As in the case where $q \equiv 1 \pmod{4}$, we have $E\mathbf{v} = (\lambda^2 - (q-1)(q+1))\mathbf{v}$ and so

$$|\lambda^2 - (q-1)(q+1)| \leq (q-1)(q+1), \\ \lambda^2 \leq 2(q-1)(q+1).$$

Hence, the absolute value of each eigenvalue of A that corresponds to an eigenvector orthogonal to the all-1s vector is bounded above by $\sqrt{2(q+1)(q-1)} \leq 2(q-1)$. Applying Lemma 9, we have

$$E(\Pi_d, \Pi_d) \leq \frac{\delta |\Pi_d|^2}{|V|} + \lambda |\Pi_d|,$$

where δ is the degree of each vertex of G .

We complete the proof by observing that $E(\Pi_d, \Pi_d) = |Q'_d|$ is the exactly the quantity that we want to bound, and then substituting the previously calculated values for δ , $|V|$ and λ into this inequality. \square

We will use the following bound on $\sum_d |\Pi_d|^2$ established in [4]².

Lemma 13. *Let P be a set of points in \mathbb{F}_q . Then we have the estimate*

$$\sum_d |\Pi_d|^2 \ll |P|^4/q + q^2|P|^2.$$

Proof of Lemma 11. We use Lemma 13 and Proposition 12 to complete the proof.

$$\begin{aligned} |Q'| &= \sum_{d \neq 0} |Q'_d|, \\ &\leq \sum_d \left(\frac{|\Pi_d|^2}{q} + 2(q-1)|\Pi_d| \right), \\ &= \left(\sum_d \frac{|\Pi_d|^2}{q} \right) + 2(q-1)|P|^2, \\ &\ll \frac{|P|^4}{q^2} + q|P|^2. \end{aligned}$$

\square

Proof of Theorem 1. For a line $l \in B(P)$, let $w(l)$ be the number of point pairs $(\mathbf{x}, \mathbf{y}) \in P^2$ such that $B(\mathbf{x}, \mathbf{y}) = l$. Note that $\sum_l w(l) = |P|^2 - |\Pi_0|$, and since for any $\mathbf{x} \in P$ there exist at most $2q-1$ points $\mathbf{y} \in \mathbb{F}_q^2$ such that $\|\mathbf{x} - \mathbf{y}\| = 0$, we have the bound $|\Pi_0| < 2|P|q$. It can be assumed that $|P| \geq 4q$; this follows from $|P| > q^{3/2}$ provided that $q \geq 16$, and for smaller values of q the theorem follows trivially by choosing suitably large constants hidden in the \gg notation. Since $|P| \geq 4q$, we have

$$\sum_{l \in B(P)} w(l) = |P|^2 - |\Pi_0| > |P|^2/2.$$

Also, $\sum_l w(l)^2 = |Q|$. By Cauchy-Schwarz,

$$|P|^4 \ll \left(\sum_{l \in B(P)} w(l) \right)^2 \leq |B(P)| \sum w(l)^2 = |B(P)||Q|.$$

Hence, by Theorem 3,

$$|B(P)| \gg \frac{|P|^4}{|P|^4/q^2 + q|P|^2}.$$

Hence, if $|P| > q^{3/2}$, then $|B(P)| \gg q^2$. \square

²See the bound on the quantity $\sum_{\mathbb{D}} \mu^2(\mathbb{D})$ in the proof of Theorem 1.5 therein, in the case when $k = 1$ and $d = 2$.

Note that, as an alternative to Lemma 13, the bound

$$(3) \quad \sum_d |\Pi_d|^2 \ll |P|^{7/2}$$

comes from a straightforward application of the Cauchy-Schwarz inequality. This is because

$$\sum_d |\Pi_d|^2 \leq |P|^2 \max_d |\Pi_d|,$$

and then the bound $\max_d |\Pi_d| = O(|P|^{3/2})$ can be obtained by constructing a set of circles of radius d centred at points of P and applying a Cauchy-Schwarz incidence bound to show that there are $O(|P|^{3/2})$ incidences between these circles and P .

If we plug this weaker bound into the proof of Lemma 11, we obtain the bound

$$(4) \quad |Q'| \ll \frac{|P|^{7/2}}{q} + q|P|^2.$$

Although this bound is not strong enough to prove Theorem 1, a careful look at the forthcoming analysis in section 4 will show that we can use (4) instead of Lemma 11. In particular, one can obtain the proof of Theorem 2 without needing to go through the extra work involved in proving Lemma 13.

4. APPLICATION TO PINNED DISTANCES

In this section, we use the bound on the bisector energy Q to deduce an upper bound on the number of isosceles triangles determined by a set of points in the plane. A simple application of the Cauchy-Schwarz inequality translates this into a lower bound on the number of pinned distances, proving Theorem 2.

One of the tools which will be needed is a weighted version of the Szemerédi-Trotter Theorem, which generalises [16, Theorem 3] to the case when the points and lines have multiplicity.

A weighted version of the Szemerédi-Trotter Theorem. Before stating and proving the incidence bound, let us first set up some notation. Let \mathcal{L} be a multiset of lines and let \mathcal{P} be a multiset of points in the plane \mathbb{F}_q^2 . When considering the set of lines in \mathcal{L} or set of points in \mathcal{P} without multiplicity, we will refer to the set as L or P , respectively. For a line $l \in L$, the weight of l is denoted $w(l)$, that is, $w(l)$ is the number of occurrences of l in the multiset \mathcal{L} . Similarly, denote the weight of $p \in P$ by $w'(p)$. Note that

$$|\mathcal{L}| = \sum_{l \in L} w(l), \text{ and } |\mathcal{P}| = \sum_{p \in P} w'(p).$$

We define the number of incidences between \mathcal{P} and \mathcal{L} to be

$$I(\mathcal{P}, \mathcal{L}) = \sum_{\mathbf{x} \in P} \sum_{l \in L} w'(\mathbf{x}) w(l) l(\mathbf{x}).$$

Lemma 14. *Let \mathcal{P} be a multiset of points in \mathbb{F}_q^2 , and let \mathcal{L} be a multiset of lines. Then*

$$I(\mathcal{P}, \mathcal{L}) \leq \frac{|\mathcal{P}||\mathcal{L}|}{q} + \left(\sum_{p \in P} w'(p)^2 \right)^{1/2} \left(\sum_{l \in L} w(l)^2 \right)^{1/2} q^{1/2}.$$

Proof. The proof given here is identical to that in Vinh's article but with the L^2 expander mixing lemma instead of the traditional one. Each line in \mathbb{F}_q^2 is described by a point in the projective plane $\mathbb{F}_q\mathbb{P}^2$. Indeed any line l is given by $l = \{(x, y) \in \mathbb{F}_q^2 : ax + by + c = 0\}$ for some (a, b, c) defined up to non-zero scalar multiples. We also have the usual embedding of \mathbb{F}_q^2 into the projective plane $(x, y) \mapsto [x : y : 1]$. Consider the graph on $q^2 + q + 1$ vertices given by points in $\mathbb{F}_q\mathbb{P}^2$, and which has as edges

$$E = \{ \{[a : b : c], [x : y : z]\} : ax + by + cz = 0 \}.$$

A straightforward calculation shows that this graph is $(q+1)$ -regular. After identifying $l \in L$ and $p \in P$ with their corresponding points in $\mathbb{F}_q\mathbb{P}^2$, the number of weighted number of incidences is

$$\sum_{l=[a:b:c] \in L} w(l) \sum_{\substack{p=[x:y:1] \in P \\ ax+by+c=0}} w'(p) = \langle w, Aw' \rangle$$

Vinh showed that the non-trivial eigenvalues of A all have size at most \sqrt{q} and thus the lemma follows from Lemma 9. \square

Bounding the number of distinct isosceles triangles. The next task is to use the weighted incidence bound to obtain an upper bound on the number of isosceles triangles determined by P . The set of isosceles triangles determined by P is defined to be the set of ordered triples

$$\Delta(P) := \{(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in P^3 : \|\mathbf{x} - \mathbf{z}\| = \|\mathbf{y} - \mathbf{z}\|, \|\mathbf{x} - \mathbf{y}\| \neq 0\}.$$

Lemma 15. *For any set $P \subset \mathbb{F}_q^2$,*

$$|\Delta(P)| \ll \frac{|P|^3}{q} + \frac{|P|^{5/2}}{q^{1/2}} + q|P|^{3/2}.$$

Proof. Define a multiset of lines \mathcal{L} to be the set of perpendicular bisectors determined by pairs of elements from $\mathbf{x}, \mathbf{y} \in P$ such that $\|\mathbf{x} - \mathbf{y}\| \neq 0$. The weight of a line $l \in L$ is the number of pairs in $P \times P$ which determine l . That is,

$$w(l) = \{(\mathbf{x}, \mathbf{y}) \in P \times P : l = B(\mathbf{x}, \mathbf{y})\}.$$

Now³, note that the number of weighted incidences $I(P, \mathcal{L})$ is precisely the quantity $\Delta(P)$. Indeed, by the definition of the perpendicular bisector

³In this particular incidence problem, we have a multiset of lines \mathcal{L} , but our set of points P is not a multiset in the true sense. That is, all of the elements $p \in P$ have weight $w'(p) = 1$.

$B(\mathbf{x}, \mathbf{y})$, a point \mathbf{z} belongs to the line $B(\mathbf{x}, \mathbf{y})$ if and only if $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \Delta(P)$. Applying Lemma 14 yields,

$$(5) \quad |\Delta(P)| \leq \frac{|P||\mathcal{L}|}{q} + |P|^{1/2} \left(\sum_{l \in L} w^2(l) \right)^{1/2} q^{1/2}.$$

The quantity $|\mathcal{L}|$ is the total weight of the lines, which is the number of pairs of elements of P whose distance is non-zero. That is,

$$(6) \quad |\mathcal{L}| = |P|^2 - |\Pi_0| < |P|^2.$$

As in the proof of Theorem 1 the quantity $\sum_{l \in L} w^2(l)$ is equal to Q , which was bounded in Theorem 3. Therefore, we have

$$(7) \quad \sum_{l \in L} w^2(l) \ll \frac{|P|^4}{q^2} + q|P|^2.$$

Combining (5), (6) and (7), it follows that

$$|\Delta(P)| \ll \frac{|P|^3}{q} + \frac{|P|^{5/2}}{q^{1/2}} + q|P|^{3/2},$$

as required. \square

Note, in particular, that

$$(8) \quad |P| \geq q^{4/3} \Rightarrow |\Delta(P)| \ll \frac{|P|^3}{q}.$$

Proof of Theorem 2. Recall that Theorem 2 states that, if $|P| \geq q^{4/3}$ then there exists a subset P' such that $|P'| \gg |P|$ and, for all $\mathbf{a} \in P'$,

$$|\{\|\mathbf{a} - \mathbf{b}\| : \mathbf{b} \in P\}| \gg q.$$

Following a familiar argument from the Euclidean pinned distances problem (see, for example [13]), it will be shown that an upper bound on the number of isosceles triangles implies a lower bound for the number of pinned distances.

For a point $\mathbf{a} \in P$, construct a family of circles \mathcal{C}_a which consists of all circles centred at \mathbf{a} with non-zero radius which contain at least one point from P . In particular, note that $|\mathcal{C}_a| < |\{\|\mathbf{a} - \mathbf{b}\| : \mathbf{b} \in P\}|$. Observe that

$$(9) \quad |\Delta(P)| = \sum_{\mathbf{a} \in P} \sum_{C \in \mathcal{C}_a} (|C \cap P|^2 - |\{(\mathbf{b}, \mathbf{c}) \in (C \cap P)^2 : \|\mathbf{b} - \mathbf{c}\| = 0\}|).$$

The next observation is that for a circle C with non-zero radius centred at \mathbf{a} and a fixed point $\mathbf{b} \in C \cap P$, there is only one point which is a distance zero from \mathbf{b} and lies on the circle C , and this point is \mathbf{b} . Indeed, it can be verified directly that the only choice of \mathbf{c} satisfying the system of equations

$$\|\mathbf{c} - \mathbf{b}\| = 0, \quad \|\mathbf{c} - \mathbf{a}\| = \|\mathbf{b} - \mathbf{a}\| \neq 0$$

is $\mathbf{c} = \mathbf{b}$.

Applying this information to (9) yields

$$(10) \quad |\Delta(P)| = \sum_{\mathbf{a} \in P} \sum_{C \in \mathcal{C}_a} (|C \cap P|^2 - |C \cap P|)$$

$$(11) \quad \geq \sum_{\mathbf{a} \in P} \sum_{C \in \mathcal{C}_a} |C \cap P|^2 - |P|^2.$$

Note also that, since there are at most $2q-1$ points in P which are a distance zero from a fixed point \mathbf{a} ,

$$\begin{aligned} \sum_{\mathbf{a} \in P} \sum_{C \in \mathcal{C}_a} |C \cap P| &\geq \sum_{\mathbf{a} \in P} (|P| - 2q) \\ &\geq \sum_{\mathbf{a} \in P} |P|/2 \\ &\gg |P|^2 \end{aligned}$$

In the second inequality it is assumed that $|P| \geq 4q$. This follows from the condition that $|P| \geq q^{4/3}$ provided that q is sufficiently large, and for small q the theorem is trivially true. Then, by Cauchy-Schwarz and (8)

$$\begin{aligned} |P|^4 &\ll \left(\sum_{\mathbf{a} \in P} \sum_{C \in \mathcal{C}_a} |C \cap P| \right)^2 \\ &\leq \left(\sum_{\mathbf{a} \in P} \sum_{C \in \mathcal{C}_a} |C \cap P|^2 \right) \left(\sum_{\mathbf{a} \in P} |\{\|\mathbf{b} - \mathbf{a}\| : \mathbf{b} \in P\}| \right) \\ &\ll (|\Delta(P)| + |P|^2) \left(\sum_{\mathbf{a} \in P} |\{\|\mathbf{b} - \mathbf{a}\| : \mathbf{b} \in P\}| \right) \\ &\ll \left(\frac{|P|^3}{q} \right) \left(\sum_{\mathbf{a} \in P} |\{\|\mathbf{b} - \mathbf{a}\| : \mathbf{b} \in P\}| \right). \end{aligned}$$

Therefore,

$$(12) \quad \sum_{\mathbf{a} \in P} |\{\|\mathbf{b} - \mathbf{a}\| : \mathbf{b} \in P\}| \geq 2c|P|q.$$

for some constant $c > 0$.

Now, define $P' := \{\mathbf{a} \in P : |\{\|\mathbf{b} - \mathbf{a}\| : \mathbf{b} \in P\}| \geq cq\}$. It remains to show that $|P'| \gg |P|$. This follows from (12), since

$$\begin{aligned} 2c|P|q &\leq \sum_{\mathbf{a} \in P} |\{\|\mathbf{b} - \mathbf{a}\| : \mathbf{b} \in P\}| \\ &= \sum_{\mathbf{a} \in P'} |\{\|\mathbf{b} - \mathbf{a}\| : \mathbf{b} \in P\}| + \sum_{\mathbf{a} \in P \setminus P'} |\{\|\mathbf{b} - \mathbf{a}\| : \mathbf{b} \in P\}| \\ &\leq \sum_{\mathbf{a} \in P'} |\{\|\mathbf{b} - \mathbf{a}\| : \mathbf{b} \in P\}| + c|P|q, \end{aligned}$$

which implies that

$$c|P|q \leq \sum_{\mathbf{a} \in P'} |\{\|\mathbf{b} - \mathbf{a}\| : \mathbf{b} \in P\}| \leq |P'|q,$$

and thus $|P'| \gg |P|$. \square

ACKNOWLEDGEMENTS

Brandon Hanson was supported by NSERC of Canada. Ben Lund was supported by NSF grant CCF-1350572. Oliver Roche-Newton was supported by the Austrian Science Fund (FWF): Project F5511-N26, which is part of the Special Research Program “Quasi-Monte Carlo Methods: Theory and Applications”. Part of this research was undertaken when the authors were visiting the Institute for Pure and Applied Mathematics, UCLA, which is funded by the NSF. We are grateful to Swastik Kopparty, Doowon Koh, Tom Robbins, Adam Sheffer and Frank de Zeeuw for several helpful conversations related to the content of this paper. Finally, we are grateful to an anonymous referee for several comments which have helped to improve the exposition of the paper.

APPENDIX A. FACTS FROM FINITE PLANE GEOMETRY

All of the results in this appendix are quite elementary and rely only on linear algebra over finite fields. However, in the interest of self-containment we have included them.

A rigid motion of \mathbb{F}_q^2 is an affine map $\mathcal{A}(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$ such that

$$\|\mathbf{x} - \mathbf{y}\| = \|\mathcal{A}(\mathbf{x}) - \mathcal{A}(\mathbf{y})\|.$$

Thus rigid motions map a circle of a given radius to another circle of the same radius. We will be interested in rotations, reflections and translations, which were defined in section 2.1.

A rotation is said to be trivial if its corresponding rotation matrix is the identity, whilst a translation by \mathbf{u} is said to be trivial if $\mathbf{u} = 0$. Note that there are no trivial reflections. Also note that the product of two rotation matrices or two reflection matrices is a rotation matrix. An obvious first remark is that rotation and reflection matrices are unitary so that rotations, reflections and translations are in fact rigid.

The rigid motions we are working with are essentially described by their fixed points:

Lemma A.1. *Any non-trivial translation has no fixed points. Any non-trivial rotation has a unique fixed point. Any reflection has a unique fixed affine line.*

Proof. That a non-trivial translation fixes no points is clear.

Suppose we have a rotation $\mathcal{R}_{R,\mathbf{u}}$ with $R \neq I$. Then \mathbf{u} is clearly fixed. If \mathbf{v} was also fixed we would have $(R - I)\mathbf{v} = (R - I)\mathbf{u}$ (where I is the

identity). However, $\det(R - I)$ is non-zero⁴ since $R \neq I$. Thus $R - I$ is invertible and $\mathbf{u} = \mathbf{v}$.

A reflection matrix $S \neq I$ has eigenvalues ± 1 . If $\mathcal{S}_{S,\mathbf{u}}$ fixes \mathbf{v} then $\mathbf{u} - \mathbf{v}$ lies in the eigenspace of 1, which is a line l . Hence, $\mathbf{v} \in l + \mathbf{u}$. \square

Two rotations $\mathcal{R}_{R_1,\mathbf{u}_1}$ and $\mathcal{R}_{R_2,\mathbf{u}_2}$ are called *complimentary* if $R_1^{-1} = R_2$. Two reflections $\mathcal{S}_{S_1,\mathbf{u}_1}$ and $\mathcal{S}_{S_2,\mathbf{u}_2}$ are called *parallel* if $S_1 = S_2$. It is a straightforward computation that the fixed lines of two parallel reflections are parallel.

Lemma A.2. *The composition of any two non-complimentary rotations is a rotation, while the composition of two complimentary rotations is a translation. The composition of any two non-parallel reflections is a rotation while the composition of any two parallel reflections is a translation. The composition of a non-trivial rotation and a translation is a rotation.*

Proof. Suppose we have rotations by R_1 and R_2 about \mathbf{u}_1 and \mathbf{u}_2 respectively. The composition is the map

$$\mathbf{v} \mapsto R_2 R_1 \mathbf{v} - R_2 R_1 \mathbf{u}_1 + R_2 \mathbf{u}_1 - R_2 \mathbf{u}_2 + \mathbf{u}_2.$$

This is a rotation provided there is a \mathbf{u} such that

$$(R_2 R_1 - I)\mathbf{u} = R_2 R_1 \mathbf{u}_1 - R_2 \mathbf{u}_1 + R_2 \mathbf{u}_2 - \mathbf{u}_2$$

which exists provided $R_2 R_1$ is not the identity. If it is the identity then the rotations are complimentary and the composition is a translation. The same proof works when R_1 and R_2 are replaced by reflection matrices as the product of two reflection matrices is a rotation matrix.

If we translate by \mathbf{u}_1 and then rotate by R about \mathbf{u}_2 then the composition is

$$\mathbf{v} \mapsto R(\mathbf{v} + \mathbf{u}_1) - R\mathbf{u}_2 + \mathbf{u}_2.$$

To show this is a rotation it suffices to find \mathbf{u} such that

$$(R - I)\mathbf{u} = R\mathbf{u}_2 - R\mathbf{u}_1 - \mathbf{u}_2$$

which can be done since $R - I$ is invertible. \square

Our primary reason for being interested in rigid motions is the relationship between reflections and their fixed lines. Observe that when \mathbf{u}' lies on the fixed line of a reflection $\mathcal{S}_{S,\mathbf{u}}$ then $\mathcal{S}_{S,\mathbf{u}} = \mathcal{S}_{S,\mathbf{u}'}$.

Lemma A.3. *Suppose $\mathbf{x} \in \mathbb{F}_q^2$ and \mathcal{S} is a reflection which does not fix \mathbf{x} . Then the fixed line of \mathcal{S} is $B(\mathbf{x}, \mathcal{S}(\mathbf{x}))$. Moreover, a line l is the fixed line of a unique reflection if and only if it is non-isotropic. If $\mathbf{y} \in \mathbb{F}_q^2$ is any point such that $\|\mathbf{x} - \mathbf{y}\| \neq 0$, then the line $B(\mathbf{x}, \mathbf{y})$ is non-isotropic and there is a unique reflection \mathcal{S} such that $\mathcal{S}(\mathbf{x}) = \mathbf{y}$ which fixes it.*

⁴Note that we use the assumption that the characteristic of \mathbb{F}_q is not equal to 2 in this calculation.

Proof. Observe that if \mathbf{u} is fixed by \mathcal{S} then

$$\|\mathbf{x} - \mathbf{u}\| = \|\mathcal{S}(\mathbf{x}) - \mathcal{S}(\mathbf{u})\| = \|\mathcal{S}(\mathbf{x}) - \mathbf{u}\|$$

so that \mathbf{u} lies on $B(\mathbf{x}, \mathcal{S}(\mathbf{x}))$. But the fixed points of \mathcal{S} form a line, so it must coincide with $B(\mathbf{x}, \mathcal{S}(\mathbf{x}))$.

Let \mathbf{u}_1 and \mathbf{u}_2 be any distinct points on the line l , which is assumed to be non-isotropic. Set $\mathbf{d} = (d_1, d_2) = \mathbf{u}_1 - \mathbf{u}_2$ so that $\|\mathbf{d}\| \neq 0$. The reflection \mathcal{S} by

$$\frac{1}{d_1^2 + d_2^2} \begin{pmatrix} d_1^2 - d_2^2 & 2d_1d_2 \\ 2d_1d_2 & d_2^2 - d_1^2 \end{pmatrix}$$

about \mathbf{u}_1 fixes l . This reflection is in fact unique. If \mathcal{S}' were another reflection fixing l then their composition would be either a rotation or a translation fixing a line. It follows that $\mathcal{S}' = \mathcal{S}$.

Finally, suppose $\mathbf{y} \in \mathbb{F}_q^2$ is distinct from \mathbf{x} . If $B(\mathbf{x}, \mathbf{y})$ is isotropic then for distinct points $\mathbf{u}_1, \mathbf{u}_2 \in B(\mathbf{x}, \mathbf{y})$ we have $\mathbf{d} = \mathbf{u}_1 - \mathbf{u}_2 = t \cdot (1, \pm i)$. Since $\mathbf{x} - \mathbf{y}$ is orthogonal to \mathbf{d} we must have that $t(\mathbf{x} \pm i\mathbf{y}) = 0$ and $\|\mathbf{x} - \mathbf{y}\| = 0$. \square

Proof of Lemma 4. Since B is non-isotropic, there is a unique reflection \mathcal{S} which fixes it. Then $\mathbf{z} = \mathcal{S}(\mathbf{x})$ and $\mathbf{w} = \mathcal{S}(\mathbf{y})$ and the result follows by rigidity. \square

We have already mentioned that rigid motions send circles to circles. In fact given two points on a circle, we now discuss when a rigid motion sends one to the other.

Lemma A.4. *Let $\mathbf{x}, \mathbf{y} \in C_r(\mathbf{u})$ for elements $\mathbf{x}, \mathbf{y}, \mathbf{u} \in \mathbb{F}_q^2$ and $r \neq 0$. There is a unique rotation \mathcal{R} fixing \mathbf{u} and sending \mathbf{x} to \mathbf{y} .*

Proof. After applying a translation if necessary we can assume $\mathbf{u} = 0$. Then we have points \mathbf{x} and \mathbf{y} with $\|\mathbf{x}\| = \|\mathbf{y}\|$. We need a rotation matrix R such that $R\mathbf{x} = \mathbf{y}$. That is, we are to solve

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

where $\mathbf{x} = (x_1, x_2)$ and $\mathbf{y} = (y_1, y_2)$. This is the same as solving

$$\begin{pmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Since $x_1^2 + x_2^2 \neq 0$ this linear equation has a unique solution. We need to check that this unique solution satisfies $a^2 + b^2 = 1$. Indeed, we can write

$$(13) \quad \begin{pmatrix} a \\ b \end{pmatrix} = \|\mathbf{x}\|^{-1} \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \|\mathbf{x}\|^{-1} \begin{pmatrix} x_1y_1 + x_2y_2 \\ x_1y_2 - x_2y_1 \end{pmatrix}$$

It follows that

$$\|(a, b)\| = \|\mathbf{x}\|^{-2} \|(x_1y_1 + x_2y_2, x_1y_2 - x_2y_1)\| = \|\mathbf{x}\|^{-2} \|\mathbf{x}\| \|\mathbf{y}\| = 1.$$

Suppose there were another rotation matrix R' with the same property. Then $R'R^{-1}$ would be a rotation matrix fixing two points, 0 and \mathbf{y} , and so must be the identity. \square

Lemma A.5. *Suppose $\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w} \in \mathbb{F}_q^2$ such that $(\mathbf{x}, \mathbf{y}) \neq (\mathbf{z}, \mathbf{w})$ and*

$$\|\mathbf{x} - \mathbf{y}\| = \|\mathbf{z} - \mathbf{w}\| \neq 0.$$

If $\mathbf{x} - \mathbf{y} \neq \mathbf{z} - \mathbf{w}$, then there is a unique rotation \mathcal{R} with $\mathcal{R}(\mathbf{x}) = \mathbf{z}$ and $\mathcal{R}(\mathbf{y}) = \mathbf{w}$, and there are no translations with this property. If $\mathbf{x} - \mathbf{y} = \mathbf{z} - \mathbf{w}$ then there is a unique translation \mathcal{T} with $\mathcal{T}(\mathbf{x}) = \mathbf{z}$ and $\mathcal{T}(\mathbf{y}) = \mathbf{w}$, and there are no rotations with this property.

Proof. Let \mathcal{T} be translation by $\mathbf{z} - \mathbf{x}$. Then $\mathcal{T}(\mathbf{x}) = \mathbf{z}$. If $\mathbf{x} - \mathbf{y} = \mathbf{z} - \mathbf{w}$ then $\mathcal{T}(\mathbf{y}) = \mathbf{w}$ and \mathcal{T} is the desired translation and it is plainly unique. Moreover, if \mathcal{R} is a rotation with $\mathcal{R}(\mathbf{x}) = \mathbf{z}$ and $\mathcal{R}(\mathbf{y}) = \mathbf{w}$ then by Lemma A.2, $\mathcal{R}^{-1} \circ \mathcal{T}$ is a non-trivial rotation fixing both \mathbf{x} and \mathbf{y} which is impossible.

Otherwise $\mathbf{x} - \mathbf{y} \neq \mathbf{z} - \mathbf{w}$ and

$$\|\mathbf{z} - \mathbf{w}\| = \|\mathbf{x} - \mathbf{y}\| = \|\mathcal{T}(\mathbf{x}) - \mathcal{T}(\mathbf{y})\| = \|\mathbf{z} - \mathcal{T}(\mathbf{y})\|.$$

Thus $\mathcal{T}(\mathbf{y})$ and \mathbf{w} lie on a common circle centered at \mathbf{z} and there is a non-trivial rotation \mathcal{R} about \mathbf{z} with $\mathcal{R}(\mathcal{T}(\mathbf{y})) = \mathbf{w}$. Then by Lemma A.2, $\mathcal{R}' = \mathcal{R} \circ \mathcal{T}$ is the desired rotation. As for uniqueness, if we had another non-trivial rotation \mathcal{R}'' then the non-trivial rotation $\mathcal{R}'^{-1} \circ \mathcal{R}''$ would fix both \mathbf{x} and \mathbf{y} which is impossible. Similarly, if \mathcal{T} is a translation with $\mathcal{T}(\mathbf{x}) = \mathbf{z}$ and $\mathcal{T}(\mathbf{y}) = \mathbf{w}$ then $\mathcal{R}'^{-1} \circ \mathcal{T}$ is a non-trivial rotation fixing both \mathbf{x} and \mathbf{y} which is impossible. \square

We are now in a position to prove the necessary lemmas from section 2.1.

Proof of Lemma 5. After a translation we can assume $\mathbf{u} = 0$. Then any point $\mathbf{v} \in \mathbb{F}_q^2$ lies on a line passing through 0. Each of these lines contains exactly $q - 1$ non-zero points and hence there are $\frac{q^2-1}{q-1} = q + 1$ lines passing through 0.

If $q \equiv 1 \pmod{4}$ then the lines through 0 which are isotropic are spanned by $(1, i)$ or $(1, -i)$ and the rest are non-isotropic. The non-isotropic lines are fixed by a unique reflection about 0. Since rotations and reflections are in bijection, there are $q - 1$ of each about 0.

When $q \equiv 3 \pmod{4}$ there are no elements of zero norm and so no isotropic lines. The rest of the analysis is as in the $q \equiv 1 \pmod{4}$ case \square

Proof of Lemma 6. Again we may translate and assume $\mathbf{u} = 0$. Any point $\mathbf{v} \in C_0(0)$ satisfies $\|\mathbf{v}\| = 0$. When $q \equiv 1 \pmod{4}$ all such \mathbf{v} are of the form $(v, \pm iv)$ so that there are $2q - 1$ or them. When $q \equiv 3 \pmod{4}$ only $\mathbf{v} = 0$ is possible. Thus we are left with $r \neq 0$. In this case fix any $\mathbf{v} \in C_r(0)$. For any other $\mathbf{w} \in C_r(0)$ there is a unique rotation about 0 taking \mathbf{v} to \mathbf{w} . When $q \equiv 1 \pmod{4}$ there are $q - 1$ such rotations and when $q \equiv 3 \pmod{4}$ there are $q + 1$ such rotations. The second claim of the theorem is immediate. \square

Lemma A.6. *Any non-trivial rotation can be decomposed into a pair of reflections:*

- (1) *when $q \equiv 1 \pmod{4}$ there are $q - 1$ decompositions;*
- (2) *when $q \equiv 3 \pmod{4}$ there are $q + 1$ decompositions.*

Any translation by \mathbf{d} with $\|\mathbf{d}\| \neq 0$ can be decomposed into a pair of reflections in q ways. A non-trivial translation by an isotropic vector cannot be decomposed into a pair of reflections.

Proof. Suppose we have a rotation $\mathcal{R} = \mathcal{R}_{R,\mathbf{u}}$. For any reflection matrix S , RS^{-1} is also a reflection matrix. Then $\mathcal{R} = \mathcal{S}_{RS^{-1},\mathbf{u}} \circ \mathcal{S}_{S,\mathbf{u}}$, and since S could be any of the reflection matrices, there are at least $q - 1$ such decompositions when $q \equiv 1 \pmod{4}$ and $q + 1$ when $q \equiv 3 \pmod{4}$. We now prove that this accounts for all such decompositions. If $\mathcal{R} = \mathcal{S}_1 \circ \mathcal{S}_2$ then \mathcal{S}_1 and \mathcal{S}_2 are non-parallel for otherwise their composition would be a translation. The reflections \mathcal{S}_1 and \mathcal{S}_2 have fixed lines l_1 and l_2 which are non-parallel and so intersect at a point \mathbf{v} . This point is fixed by \mathcal{R} and is uniquely so since \mathcal{R} is non-trivial, that is $\mathbf{v} = \mathbf{u}$. The reflection matrices S_1 of \mathcal{S}_1 and S_2 of \mathcal{S}_2 then have to satisfy $S_2 = RS_1^{-1}$ as required.

Now suppose we have a translation by a non-isotropic element \mathbf{d} . Let S be the reflection matrix such that $S\mathbf{d} = -\mathbf{d}$. Then if $t \in \mathbb{F}_q$, the composition of

$$\mathcal{S}_1(\mathbf{v}) = S\mathbf{v} - S(-t\mathbf{d}) + (-t\mathbf{d})$$

and

$$\mathcal{S}_2(\mathbf{v}) = S\mathbf{v} - S\left(\left(\frac{1}{2} - t\right)\mathbf{d}\right) + \left(\frac{1}{2} - t\right)\mathbf{d}$$

is translation by \mathbf{d} . This gives us q distinct decompositions; indeed the fixed line of the reflection by \mathcal{S}_1 is orthogonal to \mathbf{d} and passes through $-t\mathbf{d}$ and is therefore distinct for distinct values of t . Now, suppose \mathcal{S}_1 and \mathcal{S}_2 are two reflections which compose to translation by \mathbf{d} . Then \mathcal{S}_1 and \mathcal{S}_2 are parallel with common reflection matrix S about points \mathbf{u}_1 and \mathbf{u}_2 respectively. Since $\mathbf{v} + \mathbf{d} = \mathcal{S}_2 \circ \mathcal{S}_1(\mathbf{v}) = S(S\mathbf{v} - S\mathbf{u}_1 + \mathbf{u}_1) - S\mathbf{u}_2 + \mathbf{u}_2 = \mathbf{v} + S(\mathbf{u}_1 - \mathbf{u}_2) - (\mathbf{u}_1 - \mathbf{u}_2)$ we see that $S\mathbf{d} = -\mathbf{d}$ and so the decomposition is of the form we described.

Now, we observe that all pairs of reflections are now accounted for, and hence there is no way to decompose translation by a non-zero isotropic vector into a pair of reflections. From Lemma 5, it is clear that (in the $q \equiv 1 \pmod{4}$ case) there are in total $(q - 1)q$ reflections, $(q - 2)q^2$ non-identity rotations, and $(q - 1)^2$ translations by a non-zero distance. Hence, there are $(q - 1)^2q^2$ pairs of reflections, of which $(q - 2)q^2(q - 1)$ are non-identity rotations, $(q - 1)^2q$ are translations by a non-zero distance, and $(q - 1)q$ are the identity. We have that $(q - 1)^2q^2 = (q - 2)q^2(q - 1) + (q - 1)^2q + (q - 1)q$. \square

Proof of Lemma 7. Suppose first that $\mathbf{x} - \mathbf{y} = \mathbf{z} - \mathbf{w}$. Then $\mathbf{x} \neq \mathbf{z}$ for otherwise $\mathbf{y} = \mathbf{w}$. Thus translation by $\mathbf{d} = \mathbf{z} - \mathbf{x}$ is the unique translation \mathbf{x} to \mathbf{z} and \mathbf{y} to \mathbf{w} . This translation can be decomposed in q ways if \mathbf{d}

is not isotropic, and 0 ways if \mathbf{d} is isotropic. There are no other pairs of reflections with the desired property. Indeed, by Lemma A.2 and Lemma A.5, if two reflections have the desired property, then the composition of these two reflections must be a translation, and so it must be the unique translation taking \mathbf{x} to \mathbf{z} and \mathbf{y} to \mathbf{w} .

If $\mathbf{x} - \mathbf{y} \neq \mathbf{z} - \mathbf{w}$ then there is a unique rotation taking \mathbf{x} to \mathbf{z} and \mathbf{y} to \mathbf{w} . This can be decomposed in $q - 1$ ways when $q = 1 \pmod 4$ and in $q + 1$ ways when $q = 3 \pmod 4$. Similarly to the above, by Lemma A.2 and Lemma A.5, there are no other pairs of reflections with the desired property. \square

APPENDIX B. PROOF OF THE L^2 EXPANDER MIXING LEMMA

Here we give a proof of our weighted Expander Mixing Lemma, which is essentially the same as the standard proof.

Proof of Lemma 9. Write

$$f = \sum_e \langle f, e \rangle e$$

and

$$Ag = \sum_e \langle Ag, e \rangle e = \sum_e \lambda_e \langle g, e \rangle e$$

where the summation is over the eigenfunctions e of A with eigenvalues λ_e . Via Lemma 8 we have

$$\langle f, Ag \rangle = \sum_e \lambda_e \langle f, e \rangle \overline{\langle g, e \rangle} = \delta n \mathbb{E}(f) \mathbb{E}(g) + \sum_{e \neq e_1} \lambda_e \langle f, e \rangle \overline{\langle g, e \rangle}.$$

Here we have extracted the contribution from the constant function $e_1(v) = 1/\sqrt{n}$. Since $|\lambda_e| \leq \lambda$ for each $e \neq e_1$, after an application of Cauchy-Schwarz and Lemma 8 we see

$$\begin{aligned} |\langle f, Ag \rangle - \delta n \mathbb{E}(f) \mathbb{E}(g)| &\leq \lambda \sum_{e \neq e_1} |\langle f, e \rangle| |\langle g, e \rangle| \\ &\leq \lambda \left(\sum_e |\langle f, e \rangle|^2 \right)^{\frac{1}{2}} \left(\sum_e |\langle g, e \rangle|^2 \right)^{\frac{1}{2}} \\ &= \lambda \|f\| \|g\|. \end{aligned}$$

The second claim follows by taking f and g to be the characteristic functions of S and T respectively. \square

REFERENCES

- [1] N. Alon ‘Eigenvalues, geometric expanders, sorting in rounds, and Ramsey theory’, *Combinatorica* **6** (1986), no. 3, 207–219.
- [2] N. Alon, F. Chung, ‘Explicit construction of linear sized tolerant networks,’ *Discrete Mathematics*, 72(1):15–19, 1988.
- [3] J. Beck, ‘On the lattice property of the plane and some problems of Dirac, Motzkin and Erdős in combinatorial geometry’, *Combinatorica* **3** (1983), no. 3–4, 281–297.

- [4] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan and M. Rudnev ‘Group actions and geometric combinatorics in \mathbb{F}_q^d ’, *arXiv:1311.4788*, (2013).
- [5] R. Brualdi, S. Mellendorf, ‘Regions in the complex plane containing the eigenvalues of a matrix,’ *American Mathematical Monthly*, (1994), 975–985.
- [6] J. Chapman, M. Erdoğan, D. Hart, A. Iosevich and D.Koh, ‘Pinned distance sets, k-simplices, Wolff’s exponent in finite fields and sum-product estimates’, *Math. Z.* **271** (2012), no. 1-2, 63–93.
- [7] L. Guth and N. H. Katz, ‘On the Erdős distinct distance problem in the plane’, *arXiv:1011.4105*, (2010).
- [8] H. Helfgott and M. Rudnev, ‘An explicit incidence theorem in \mathbb{F}_p ’, *Mathematika* **57** (2011), no. 1, 135–145.
- [9] A. Iosevich and M. Rudnev, ‘Erdős distance problem in vector spaces over finite fields’, *Trans. Amer. Math. Soc.* **359** (2007), no. 12, 6127–6142.
- [10] T. G. F. Jones, ‘Further improvements to incidence and Beck-type bounds over prime finite fields’, *arXiv:1206.4517*, (2012).
- [11] B. Lund and S. Saraf, ‘Incidence bounds for block designs’, *arXiv:1407.7513*, (2014).
- [12] B. Lund, A. Sheffer, and F. de Zeeuw, ‘Bisector energy and few distinct distances’, *arXiv:1411.6868*, (2014).
- [13] J. Pach and G. Tardos, ‘Isosceles triangles determined by a planar point set’, *Graphs Combin.* **58** (2002), no. 4, 769–779.
- [14] S. Roman, *Advanced linear algebra*. Springer, 2007.
- [15] J. Solymosi, ‘Incidences and the spectra of graphs’, *Combinatorial Number Theory and Additive Group Theory*, Springer, 2009, 299–314.
- [16] L. A. Vinh, ‘The Szemerédi-Trotter type theorem and the sum-product estimate in finite fields’, *European J. Combin.* **32** (2011), no. 8, 1177–1181.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO, ONTARIO, CANADA
E-mail address: `bhanson@math.utoronto.ca`

DEPARTMENT OF COMPUTER SCIENCE, RUTGERS, THE STATE UNIVERSITY OF NEW JERSEY, NJ
E-mail address: `lund.ben@gmail.com`

JOHANN RADON INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS, AUSTRIAN ACADEMY OF SCIENCES, 4040 LINZ, AUSTRIA
E-mail address: `o.rochenewton@gmail.com`